

cPacket Networks
2061 Landings Drive
Mountain View, CA 94043
www.cpacket.com

For more press information contact:
Abigail Johnson/Paul Michelson
Roeder-Johnson Corporation
+1 (650) 802-1850 FAX: +1 (650) 593-5515
<http://email.roeder-johnson.com>

For more customer information contact:
cPacket Networks
Mountain View, CA
+1 (650) 969-9500 FAX: +1 (650) 969-4900
info@cpacket.com

CPACKET TECHNOLOGY PROTECTS SHOW-FLOOR NETWORK AT INTEROP FOR THIRD TIME

Reference Hardware that Showcases cPacket's 20 Gig "Complete Packet Inspection" Chips Insulates Trade Show Good Guys from the Bad Guys - and Each Other

MOUNTAIN VIEW, CA OCTOBER 17, 2007 - cPacket Networks today announced that its complete packet inspection technology will be used for the third Interop conference in a row to protect show participants and organizers from malicious or unintended disruptions in the show network. The company will install in-line monitoring probes at 16 links in the network operating center of Interop.

Each probe is capable of inspecting both the headers and payload (data) of all traffic flowing through a link, down to the bit level, and offers the operator a variety of responses to non-conforming traffic. The probes themselves are reference designs for cPacket's unique "complete packet inspection" chips, which the company markets to network equipment original equipment manufacturers (OEMs). The widely-attended show is being held in New York City from October 22nd through 26th.

"We have a number of stringent requirements for a tradeshow network," said Mike Pennacchi, InteropNet Lead Network Engineer. "We need to install the network virtually overnight, ensure that it is up constantly, and protect it both from attacks, and from applications simply 'gone wild.' cPacket has proven invaluable in making this happen." The Interop network serves exhibitors, presenters, attendees, registration, classrooms, and the press, among others.

cPacket first demonstrated its technology at the New York Interop in late 2006, with four demonstration prototypes. The 16 units being provided this time reflects the desire of the show's network administrators to have much greater situational awareness. The show, which attracts top industry professionals, is considered a particularly inviting and "target rich" environment for network disruption and attacks, as its network addresses and the show timing are well known in advance, to the hackers of the world.

According to Pennacchi, cPacket's probes meet three very important needs in the monitoring and troubleshooting of the "InteropNet." "We are able to monitor the traffic, capture suspicious packets, and drop those that have no business being on our network," he said. The design of the probes allows them to literally be dropped anywhere in the network to provide visibility and enforcement down to every bit in every packet flowing through that link. Added Glenn Evans, Interop Lead Engineer, 2004-2007, about the technology: "The situational awareness, responsiveness, control, and security that it provides us on behalf of our network and users has far surpassed my expectations."

Complete packet inspection is cPacket's term for a process where 100% of the information flowing through a network link is inspected and analyzed in real time, even on networks running at 20 gigabits per second. Conforming data is allowed to pass, while non-conforming data can be redirected,

dropped, or rate-limited. It is called “complete” because it analyzes both the protocol header fields and payload content and is able to take action on specific traffic profiles with surgical precision.

cPacket has developed an economical chip that performs this complete packet inspection, at wire speeds up to 20 gigabits per second. The new silicon technology results in a 10-to-1 improvement in packet processing speeds, at about one-tenth the costs. The resulting 100-to-1 improvement in cost-performance permits situational awareness and rapid response to be integrated pervasively into the network infrastructure, down to the port level, without introducing the complexity, cost, or performance bottlenecks that characterize current technologies.

The 16 demonstration systems installed in the Interop network operating center are reference designs built by cPacket to showcase their chip, and the units are fully-functioning network “visibility and enforcement” appliances. The small devices provide reports that are consolidated in a management console, and can be accessed remotely from a Web browser, providing an extremely easy-to-use and intuitive interface.

According to cPacket founder and CEO Rony Kay, the simplicity and high performance of the chip will enable system designers to add complete packet inspection economically to existing or future designs of network switches, monitoring probes, and security appliances. “Situational awareness and control of network traffic is increasingly required pervasively throughout the network, particularly at the ‘local’ level of the access and aggregation layers,” said Kay. “Now, for the first time, this is both economically and technically feasible, and strategically compelling, as the Interop demonstration shows.”

About cPacket

cPacket Networks is an emerging leader in chips and technologies that offers breakthrough, “complete” packet inspection, at a fraction of the complexity, power, or cost of preexisting approaches. It provides manufacturers of routers, switches and other network appliances a low-impact means to easily drop game-changing, wire-speed active network traffic analysis and response directly into their existing or planned designs - whether targeted at the service providers, the enterprise, or the small office. The exploding use of networks for media-centric applications makes the availability of truly pervasive deep packet inspection timely and crucial.

cPacket was founded in 2003 and is located in Mountain View, CA. For more information, visit www.cpacket.com.

Editors, note: All trademarks and registered trademarks are those of their respective companies.

Keywords: “complete packet inspection”; “deep packet inspection”; “network security”; “network monitor”; “network probe”; “network protection”; “situational awareness”; “traffic analysis”; “wire speed”; “chip”.

Additional background information is available at www.roeder-johnson.com.

See also: “cPacket Executive Says Network Security Falls Far Short; Requires Pervasive, Multi-tiered Approach With a Local Focus”, September 19, 2007, <http://www.roeder-johnson.com/RJDocs/CPclasschip0919.html>